

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of)

Case No. 19-mj-119-JFJ

INFORMATION ASSOCIATED WITH O.WUTTKE@SCHRNIDT-
CLEMENS.COM THAT IS STORED AT PREMISES CONTROLLED
BY GOOGLE LLC.

SEARCH AND SEIZURE WARRANT

To: SA Evan Held or any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment "A":

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment "B":

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

8-21-19

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge Jodi F. Jayne
(name)

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for _____ days (not to exceed 30).

☐☒ until, the facts justifying, the later specific date of 8/6/2020.

Date and time issued:

8-7-19


Jodi F. Jayne
Judge's signature

City and state: Tulsa, Oklahoma

U.S. Magistrate Judge Jodi F. Jayne

Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.: 19-MJ-119-JFJ	Date and time warrant executed: 08/07/2019 at approx. 4:17PM	Copy of warrant and inventory left with: Google LLC
Inventory made in the presence of : FBI Special Agent Alan T. Siska		
Inventory of the property taken and name of any person(s) seized: One (1) PDF file and one (1) ZIP file containing data associated with account o.wuttke@schnridt-clemens.com.		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: <u>09/19/2019</u>	<div style="text-align: center;">  _____ <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 10px;"> Evan D. Held, FBI SA _____ <i>Printed name and title</i> </div>	

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC (the “Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California and applies to all content and other information within the Provider’s possession, custody, or control associated with the e-mail account O.WUTTKE@SCHRNIDT-CLEMENS.COM (the “Subject Account”).

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 24, 2019, the Provider is required to disclose the following information to the government for each account listed in Attachment A:

1. *E-mail Content.* All e-mails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each e-mail, the data and time at which each e-mail was sent, and the size and length of each e-mail), limited to items sent, received, or created between February 26, 2019 and present;
2. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.
3. *Google services information.* The files and contents with the account related to Google services, including Google Drive, Google Docs, Google Photos, Google Calendar, Google Chats, Google Hangouts, Google Photos, Web and Search History, and Google Payments.
4. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username,

address, telephone number, alternate e-mail addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

5. *Search and web history records.* All records relating to web and application activity history (including search terms), device information history, and location history.
6. *Device information.* Any information identifying the device or devices used to access the Subject Account, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identify Numbers (“MEIN), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the Subject Account.
7. *Information Regarding Linked Accounts, Including Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Account, including specifically by cookie, Google Account ID, Android ID, or other account or device identifier (the “Linked Accounts”).

- a. The following information regarding the customers or subscribers of the Linked Accounts:

1. Names (including subscriber names, user name, and screen names);
 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 3. Local and long distance telephone connection records;
 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol addresses and port numbers) associated with those sessions;
 5. Length of service (including start date) and types of service utilized;
 6. Telephone or instrument numbers (including MAC addresses);
 7. Other subscriber numbers or identities (including the registration Internet Protocol address); and
 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
8. *Location Data.* All location data associated with the Subject Account, including GPS data, cell site/cell tower triangulation/trilateration, and Wi-Fi location, including the GPS coordinates and dates and times of all location recordings.
9. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.
10. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

11. *Preserved or backed up records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. Section 2703(f) or otherwise.

Google is further ordered to disclose the above information to the Government within 14 days after service of this warrant.

II. Information to be seized by the government

1. All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer intrusions), 1343 (wire fraud), 1956 (money laundering), and 371 (conspiracy),(collectively the “Subject Offenses”), including information pertaining to the following matters:

- a. E-mail communications with the Victim Company;
- b. Any information related to the Victim Company;
- c. Information identifying the user or the location of the user of the Subject Account, and the individual involved in the Subject Offenses, including photographs or videos depicting the user of the Subject Account, communications with individuals that the user of the Subject Account trusts, which reveal his/her identity to include information that can be used to ascertain his/her identity, such as travel information or receipts for online purchases or other communications with social network websites or third party service providers;
- d. Communications of the user of the Subject Account with co-conspirators and others about the Subject Offenses, including but not limited to obtaining unauthorized access to the data from computer systems, reconnaissance of victim computer systems, victim selection and targeting, malicious software, software vulnerabilities, malicious domains, phishing e-mails, and monetizing stolen personal and computer system information belonging to other individuals, and communications and other data identifying such co-conspirators;
- e. Communications and documents concerning the wiring or transferring of funds between bank accounts;

- f. Phishing e-mails seeking to induce individuals to click on hyperlinks, download attachments, or otherwise take action to infect victim systems with malware, and test versions of the same;
- g. Evidence concerning the user's technical expertise;
- h. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- i. Information regarding the registration of other e-mail accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, and payment for such online facilities or services; and
- j. Evidence concerning any other online accounts or any computer devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.